REMARKS

In the Official Action mailed on **2 June 2006**, the Examiner reviewed claims 1-11, 13-29, 31-47, and 49-54. Claims 1, 4, 5, 8, 9, 13, 15, 16, 18, 19, 22, 23, 26, 27, 31, 33, 34, 36, 37, 40, 41, 44, 45, 49, 51, 52, and 54 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bruce Schneier (*Applied Cryptography 2nd Edition*, Oct. 1995, John Wiley & Sons Pub. pages 43-57, hereinafter "Schneier") in view of Medvinski et al (*Public Key Utilizing Tickets for Application Servers*, hereinafter "Medvinski") and Kohl et al (*The Kerberos Network Authentication Service, Network Working Group Request For Comments (RFC)* 1510, Sept. 1993; hereinafter "Kohl"). Claims 14, 17, 32, 35, 50, and 53 were rejected as being unpatentable over Schneier in view of Medvinski and Official Notice (hereinafter "ON"). Claims 2, 3, 6, 7, 10, 11, 20, 21, 24, 25, 28, 29, 38, 39, 42, 43, 46, and 47 were rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Medvinski and Sirbu et al (*Public Key Based Ticket Granting service in Kerberos*, hereinafter "Sirbu") and ON.

Rejections under 35 U.S.C. §103(a)

Independent claims 1, 19, and 37 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Medvinski and Kohl.

Examiner avers in both the instant office action and the previous office action, that "Medvinski teaches the use of a secret key with a limited lifespan intended to reduce KDC vulnerability on page 57: 'Key Expiration'."

Unfortunately, Applicant failed to find the reference "Medvinski, page 57: 'Key Expiration'" during the procedure of previous office action response. Applicant has communicated with Examiner in an attempt to obtain aforementioned reference. However, by far the reference has not been provided.

Applicant respectfully points out that the session key with a limited lifespan taught by Schneier on page 47, Sec. 3.1 "Key Exchange" is the same type of session key taught by Kohl in Kerberos. These session keys are typically used

for only one communication session, thereby having a limited lifespan. In this perspective, Applicant acknowledges that the session key and the temporary secret key of the instant application are both communication keys with limited lifespan.

However, the temporary secret key of the instant application not only has a limited lifespan, but also a **short lifespan**. This is because the temporary secret key is a short-term secret that becomes invalid after a short time period (see Page 9, lines 23-26). Note that such a short-term secret is essential in the instant application as an approach to reduce the vulnerability associated with the prior art long-term secret. In contrast, a session key in the combined system of Schneier, Medvinsky, and Kohl does not need to have a short lifespan, rather the limited lifespan is decided by the duration of the server-client communication session, which **can be arbitrarily long**.

Furthermore, a session key is different from the temporary secret key of the instant application in the following aspects. First of all, the secret key is shared between a principal and the KDC, and stored at the KDC and the principal. In contrast, the session key is generated at the time that two principals (e.g., a client and a server) need to establish communications, and then shared by the two principals. Secondly, the session is typically generated by the KDC by request of a principal, while the secret key is typically generated by the principal. Thirdly, the lifetime or lifespan of the session key is associated with a communication session, while the lifetime of the secret key is not associated with a communication session. Lastly, the secret key is used to create a ticket by "encrypting an identifier for the client and the session key with the temporary secret key," in the instant application, while the session key is used for direct communication between the client and the server.

Kohl describes the Kerberos network authentication system, which provides a means of verifying the identities of principals on an open network. Kerberos allows a client to obtain a "ticket" from a KDC which enables the client to (a) authenticate itself to a server and (b) initiate a secure session with the

server. Note that Kerberos uses a **long-term secret key** (with "**long lifetime**") which is shared between the KDC and the server to seal the ticket (see Kohl, section 1.3, definitions for "secret key" and "ticket").

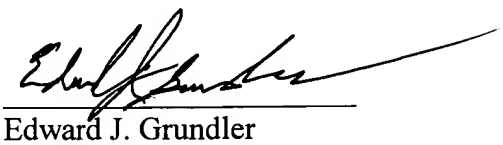
Accordingly, Applicant has amended independent claims 1, 19, and 37 to clarify that the temporary secret key of the instant application becomes invalid after a short time period, therefore is a short-term secret. Applicant additionally adds the limitation that the temporary secret key is shared between the server and the KDC to further distinguish it from a session key. These amendments find support on page 9, lines 24-26, and page 11, lines 10-14.

Hence, Applicant respectfully submits that independent claims 1, 19, and 37 as presently amended are in condition for allowance. Applicant also submits that claims 2-11 and 13-18, which depend upon claim 1, claims 21-29 and 31-36, which depend upon claim 19, and claims 38-47 and 49-54, which depend upon claim 37, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 

Edward J. Grundler
Registration No. 47,615

Date: June 21, 2006

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1663
FAX: (530) 759-1665
Email: edward@parklegal.com